The Office of General Counsel

THIS PRESENTATION

IS CLASSIFIED

TOP SECRET//COMINT//[redacted]

General Principles of Law

- **Principle #1: Authority**
  (What is the authority to do my job?)

- **Principle #2 Restrictions**
  (Is the authority restricted in any way?)

Constitution
Fourth Amendment

- Protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.

- Requires probable cause for a search warrant.

Supreme Court Cases

- **Olmstead v. U.S. (1928)**
- **Katz v. U.S. (1967)**

Operation Shamrock: 1945-1975

- NSA received copies of international telegrams to, from, and transiting the U.S.
- Included virtually all international telegrams carried by major telecom carriers.
- In later years, 150,000 telegrams per month reviewed by NSA analysts
- Probably the largest governmental interception program affecting Americans ever undertaken

Project Minaret: 1967-1973 (The Watch List)

- **Names of U.S. persons used systematically as basis for selecting messages**
- **Foreign influence on Domestic Antiwar and Civil Rights Activists**

Narcotics Collection: 1970-1973

- **Telephone Links between the U.S. and South America collected**
- **Used Names of U.S. persons**
- **Obtained Communications that Law Enforcement could not acquire under Title III**

The Problem…

Congressional Inquiries
Church/Pike Committees

Information TO, FROM, and ABOUT U.S. Citizens was:

Improperly Collected
Improperly Retained
Improperly Disseminated

Results of Church Committee and Other Investigations

- Termination of illegal collection activities
- Executive Order requiring the establishment of procedures relating to U.S. person information
- Greater Executive and Legislative Oversight

Congressional/Executive Response to IC Abuses

- **Federal Law** → **Foreign Intelligence Surveillance Act** (as amended)
- **Executive Order** → **E.O. 12333 Intelligence Activities**
- **Regulations and Procedures** → **DoD 5240.1-R and Classified Annex**
  USSID SPOO18 (USSID 18)
  Minimization Procedures

End of Module One

The Foreign Intelligence Surveillance Act (FISA)

- The FISA, was originally passed in 1978.
- Most recently amended in the FISA Amendments Act (FAA) of 2008.
- Defines "electronic surveillance" and requires an order from the Foreign Intelligence Surveillance Court (FISC) to conduct such surveillance.
- As amended, by the FAA, requires that the USG obtain a court order to conduct electronic surveillance against US persons either in the US or abroad.

Definitions

- Electronic Surveillance
- U.S. Person
- Foreign Power
- Agent of a Foreign Power
- Contents

FISA
"Electronic Surveillance"

- f(1): acquisition of communications of particular known USP inside the US by targeting that person
- f(2): acquisition of wire communication to or from a person in the US if acquisition occurs inside the US
- f(3): acquisition of radio communications if all parties to the communication are located inside the US
- f(4): monitoring in the US to acquire information other than from a radio or wire communication

Definitions -- U.S. Persons

- U.S. Citizen
- Permanent Resident Alien (Green Card Holder)
- Corporations (incorporated in the U.S.)
- Associations (primary membership composed of U.S. persons)
- U.S. flagged ships/aircraft

Definitions -- Foreign Power

- A foreign government or any component thereof
- A faction of a foreign nation
- An entity openly acknowledged to be directed or controlled by a foreign government(s)
- a group engaged in international terrorism
- a foreign based political organization

Definitions -- Agent of a foreign power

- **An officer or employee of a foreign power**

- **A spy, terrorist, saboteur, aider/abettor, or conspirator**

Definitions

Communications

Any information conc-
cerning the identity of
the parties to such
communications
OR

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

-- Contents

"Substance"

"Purport"

"Meaning"

"Existence"

FISA Amendments Act of 2008

- Became law in July 2008
- Applies to targets overseas
- Sections 702/703/704/705

FISA Amendments Act of 2008
Section 702

- Authorizes the USG to gather foreign intelligence by targeting foreign persons reasonably believed to be outside the US with authorization jointly executed by the AG and DNI.

- The government must employ targeting procedures and minimization procedures which comply with the statute and which are reviewed by the FISC.

- Prohibits "reverse targeting".

FISA Amendments Act of 2008 Section 703

- Authorizes "electronic surveillance" against a USP reasonably believed to be outside of the US, but --
- An order from the FISC is required.
- Target must be a "foreign power", "agent of a foreign power", or officer or employee of a foreign government.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

FISA Amendments Act of 2008 Section 704

- Authorizes "other acquisitions" targeting US persons overseas – but

- An order from the FISC is required.

- The FISC does not review surveillance techniques.

FISA Amendments Act of 2008
Section 705

- 705(a) – a judge may simultaneously authorize acquisitions conducted both inside and outside of the US against a USP overseas (703 and 704).

- 705(b) – if there is an existing FISA order authorizing surveillance of target inside of the US, the AG can authorize targeting while the USP is reasonably believed to be outside of the US.

FISA Procedures

- Establishes the Foreign Intelligence Surveillance Court
- Provides criteria/requirements for applications
- Establishes Congressional Oversight

E.O. 12333
United States Intelligence Activities

- **Provides goals, directions, and responsibilities for the Intelligence Community**
- **Defines NSA's responsibilities (Part 1.12(b)**
- **Requires each agency to have AG- approved procedures, for collection, processing and dissemination of U.S. person information**

E.O. 12333
United States Intelligence Activities

- **Provides goals, directions, and responsibilities for the Intelligence Community**
- **Defines NSA's responsibilities (Part 1.7(c))**
- **Requires each agency to have AG- approved procedures, for collection, processing and dissemination of U.S. person information**

E.O. 12333
United States Intelligence Activities

- **Collection, Processing, and Dissemination of Signals Intelligence for National Foreign Intelligence Purposes.**
- **Collection, Processing, and Dissemination for Signals Intelligence for Counterintelligence Purposes.**
- **SIGINT Support for Military Operations.**
- **Information Assurance.**

REGULATIONS

DoD 5240.1-R (1982)

Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons

NSA/CSS Policy 1-23

Procedures Governing the Activities of NSA/CSS that Affect U.S. Persons

End of Module Two

(U//~~FOUO~~) FAA Sections 703, 704, & 705 Minimization Procedures

(U//~~FOUO~~) Anyone targeting US persons located outside of the US under FAA is required to read and be familiar with the minimization procedures

(U) The Overall Classification of this presentation is TOP SECRET//COMINT//[redacted]

(U) Requirements

FAA Sections 703, 704, & 705

(U) The FAA may authorize collection against:

- ✓ A US person
- ✓ Reasonably believed to be outside of the US
- ✓ To acquire foreign intelligence information

(U) Limitations

NSA Surveillance Under Sections 703, 704, and 705

(U) NSA CANNOT use FAA authorities to target:

- Anything/Anyone in the US

(U//~~FOUO~~) NSA FAA data CANNOT be:

~ Accessed without being properly trained on NSA's FAA minimization procedures

~ Processed at locations other than those approved by SID

(U) *FISA Amendments Act of 2008*

Section 703

- (U) An order from the FISC to target a US person reasonably believed to be outside the US
- (U) Authorizes "electronic surveillance" or the acquisition of stored electronic communications or stored electronic data
- (U) Authorization for up to 90 days

(U) *FISA Amendments Act of 2008*
Section 704

- (U) An order from the FISC to target a US person reasonably believed to be outside the US
- (U) Authorizes "other acquisitions" targeting US persons overseas (techniques are not described to the court)
- (U) Authorization for up to 90 days

(U) *FISA Amendments Act of 2008*

Section 705

(U) Section 705 has two parts, 705(a) and 705(b).

- (U) 705(a) authorizes the Government to request, and a judge to issue a single order authorizing 703 and 704 surveillance

- (U) 705(b) authorizes the AG to approve surveillance of a US person overseas if the FISC has already issued an order authorizing electronic surveillance or physical search against that US person in the US

NSA Minimization Procedures for Collection Under FAA Sections 703, 704, & 705

(U//FOUO) Minimization Procedures need to be Followed Unless…

- (U//FOUO) To protect US National Security, life or property, or for Law enforcement purposes – NSA may deviate from Standard Minimization Procedures with AG approval (coordinate in advance with NSA OGC)

- (U//FOUO) If advance coordination is not feasible and NSA needs to act in order to protect against immediate threat to human life – consult with NSA OGC who must report any such action within 7 days to DOJ

- (U) **if you believe you must deviate from the procedures, YOU MUST GO TO NSA/OGC FIRST!!!!**

NSA Minimization Procedures for Under FAA Sections 703, 704, & 705

(U) Collection

(S//SI//)

- NSA must terminate collection promptly if NSA learns that a targeted US person is located in the US

- Collection against a US person in the US may only be reinstated in accordance with the FISA

- NSA may resume collection if the target departs the US during the life of the order

- Selectors for 704 and 705 surveillances may be tasked [redacted]

NSA Minimization Procedures Under FAA Sections 703, 704, & 705

(U) Processing

(U//~~FOUO~~) Searches or reviews of collected materials must be designed, to the extent operationally possible, to minimize the risk of returning data concerning unconsenting US person 's who are not the target of authorized surveillance

[redacted]

[redacted]

NSA Minimization Procedures Under FAA Sections 703, 704, & 705

(U) Retention

(S//SI//[redacted]) The following communications shall be destroyed upon recognition unless the AG authorizes retention:

- Inadvertent collection of communications while the target enters the US
- Inadvertent collection of communications in which all the communicants are in the US
- Inadvertent collection of communications in which all the communicants are US persons who are not authorized targets

(U) AG Destruction Waiver

(S//SI//[redacted])

Inadvertent Collection:

- All communicants inside the US
- All communicants are US person's who are not authorized targets
- The authorized target is in the US

Data shall be destroyed unless the AG determines that the communication contains:

- Significant foreign intelligence
- Evidence of a serious crime
- Information related to a threat of serious harm to life or property
- Technical information about a communications vulnerability

(S//SI//[redacted])

(U) Without AG Destruction Waiver

(S//SI//[redacted])

Inadvertent Collection:

- Of US domestic communications
- Against an unauthorized target

Even without a Destruction Waiver, technical data concerning such communications may be retained for collection avoidance purposes

(S//SI//[redacted])

NSA Minimization Procedures Under FAA Sections 703, 704, & 705

(U) Retention

- (U//~~FOUO~~) NSA may retain FAA data in databases for up to 5 years without additional authorization

- (U//~~FOUO~~) NSA's SIGINT Director may authorize retention for a longer period in response to an authorized foreign intelligence or counterintelligence requirement

[redacted]

(U) Incident Reporting

(U//~~FOUO~~) All incidents should be reported at the time of recognition AND again in the IG Quarterly report

(U//~~FOUO~~) Incidents include:

- Inadvertent and incidental collection
- Unauthorized targets
- Collection continued on targets inside the U S
- Unauthorized access to data:
  - By unauthorized personnel
  - By untrained personnel
  - At non-SID-approved locations
- Inappropriate storage, labeling, or handling

(U) Requirements for Data Access

(U//~~FOUO~~) To gain access to data both the individual user and the location must be certified

- The user must:
  - Complete this training (renewing it every two years)
  - Maintain current Annual Intelligence Oversight readings
  - Work under DIRNSA's full operational & technical control
  - Have a mission need

- The location must:
  - Operate under DIRNSA's full operational & technical control
  - Possess a delegated mission
  - Have SID approval for access to FAA data
  - Have an established oversight infrastructure

FAA Sections 703, 704, & 705

(U) Where to go for Help

(U//~~FOUO~~)

OGC: DL GC_FISA

(after hours contact NSOC SOO to get in touch with OGC)

Oversight and Compliance: DL FISATEAM

Targeting Mission Management (TMM): DL OPSDICTS

Documents Available at SV1 Homepage: ('go SV')

- For the Minimization Procedures document
- Comparison charts of 703/704/705 orders
- Specific targets authorized under these sections

USSID SP0018

Legal Compliance and Minimization Procedures

- **Main body of SPOO18 Compilation of responsibilities from the FISA, E.O. 12333, and DoD Regulation 5240.1-R as they apply to the U.S. SIGINT system**
- **covers collection, processing, retention, and dissemination**

What is "Collection"?

- Targeting a SPECIFIC COMMUNICANT (e.g. a terrorist, a foreign minister, a computer hacker)

- Collecting based upon SUBJECT MATTER (e.g. nuclear proliferation, oil sales, economics)

Targeting Specific Communicants
SPOO18 Section 4

The Four Rules

- No [redacted] without Attorney General approval
- No U.S. Persons in the U.S. without a Court Order
- No U.S. persons outside the U.S. without a Court Order
- Foreign persons outside the U.S. -- fair game

Targeting by Subject Matter USSID SPOO18 Section 5

- Selection terms that:
  - have intercepted or
  - are likely to intercept
- U.S. Person communications
- MUST BE DESIGNED
  - (to the greatest extent practicable under the circumstances)
- to DEFEAT communications that
- do not contain foreign intelligence

Targeting Issues

Presumptions

(If no other information is available)

- In the U.S., then U.S. person
- Outside the U.S., then foreigner

Targeting Definitions

Targeting U.S. Persons

- INADVERTENT (Did not know is a U.S. Person)
- INCIDENTAL (Legitimate foreign target; as a by product NSA acquires U.S. Person information/communications)
- REVERSE (Target foreign entity to intentionally acquire U.S. Person information/communications)

USSID SPOO18 Dissemination

- **Allow access to non-minimized raw traffic voice/data database**
- **Provide copy of a non-minimized piece of raw traffic**
- **Disclose (orally or in writing) the contents of non-minimized raw traffic**
- **Disclose (orally or in writing) the identity of a U.S. person contained in an NSA product**

USSID SPOO18 Dissemination

Authorized Recipients of Raw Traffic

THE SIGINT PRODUCTION CHAIN

People who Collect Raw Traffic

People who Process Raw Traffic

People who Retain Raw Traffic

People who Manage the SIGINT Process

People who do Oversight of the SIGINT Process

USSID SPOO18 Dissemination

Examples of Non-SIGINT Production Personnel

- A Customer in Another Agency (e.g. CIA, FBI)
- Another Agency's Liaison Representative to NSA
- Non-SIGINT producing NSA Organizations or Personnel (e.g Security (Q), Personnel (MD))
- NSA Employees Detailed/Assigned to Another Agency (e.g. CIA/TMO, IOTC)
- Any person not necessary to Produce the SIGINT Product

End of Module Three

Questions?

- Who is the target?
  - U.S. Person or Non-U.S. Person
- Where is the target?
  - In the U.S. or Outside the U.S.
- What kind of communications will be collected?
  - Private (e-mail, wire, cell, encrypted) or Non-Private
- How will the communications be collected?
  - Passively or Actively
- Where will the communications be collected?
  - In the U.S. or Outside the U.S., or in International Waters, or from Outer Space

Questions?

Office of General Counsel

(Operations/Intel Law)



NSOC has an attorney on call 24/7!

Database Access Briefing

USSID SP0018 and Raw Traffic Databases

(U//~~FOUO~~)Contact O&C or the OGC if you have questions about this material

<u>NSA SID Oversight and Compliance (Database Team):</u> [redacted] (nsts)
dl u18dbtarget

<u>NSA SID Oversight and Compliance (Reporting Team):</u> [redacted] (nsts),
[redacted]
dl ussid18

(U//~~FOUO~~) Contact O&C or the OGC if you have questions about this material

NSA Office of the General Counsel (Ops):

(nsts)

(for UNIX systems)

dl gcops (for NT users)

(U//FOUO) Module 5

Administration and Background

(U//~~FOUO~~) Briefing Lifespan

<u>2 Years</u> – With use of USSID SP0018 sensitive databases

<u>6 Months</u> – Without use of USSID SP0018 sensitive databases

Why is this training required?

This training covers access to and use of "Raw SIGINT" data and databases.

Raw SIGINT is: Results of collection BEFORE the information has been evaluated for foreign intelligence AND minimization purposes, per USSID CR1610.

"Analysts are not permitted … to roam freely in the universe of collected communications, examining messages which are not directly related to their assigned tasks."

-Office of Intelligence Policy and Review

Raw SIGINT access is restricted to those within a SIGINT Production Chain as defined by USSID CR1610.

There is no single "SPC".

There are SPCs at various levels from organic SIGINT assets in the field through the NSA Product Line level.

Raw SIGINT databases contain completely innocent U.S. person communications and non-foreign intelligence information as well as FI.

To protect the privacy rights of U.S. citizens, Department of Justice has determined searches of these databases are a collection/targeting activity.

~~Confidential//X1~~

Database Queries = collection/targeting

Dictionary Tasking = collection/targeting

Protecting U.S. Persons' rights is only half the story. USSID SP0018, section 5.1 states that analysts must also ensure, to the greatest extent possible, that queries only target Foreign Intelligence.

Sharing of SIGINT

In this age of data and information sharing, we must remain mindful of the current regulations that prohibit the casual sharing of SIGINT.

E.O.12333, section 2.3 specifically addresses this.

Targeting for Personal Purposes

If you know someone is using the SIGINT system for personal purposes, <u>**YOU**</u> have the responsibility to report the activity.

Auditing Requirements

USSID CR1610 Annex A details auditing requirements for certain raw SIGINT systems. This auditing meets Department of Justice mandates for NSA's operations.

Derivative Databases

If data is saved into another file or database, that derivative database must have the same access, auditing and retention issues that the originating database held

Access and Retention

USSID SP0018, Section 6

- 5 Years on-line
- Up to 10 years off-line—request for historical searches made to OIPR
- Some retention exceptions
- Recognizes intrusiveness of SIGINT
- FISA Data: Depends upon nature of data –check USSID SP0018, Annex A, and/or call SV

Accountability of Access

NSA must account for:

1. Who uses SIGINT databases
2. What purpose
3. From what location
4. Under what controls

Therefore, accesses must be re-justified if:

1. You Change Offices or Mission
2. You Change Locations
3. You Change Auditors
4. Your Account Lapses Due to Inactivity for 90 days

End of Module 5

(U//FOUO) Module 6

Protections and Restrictions

(U//~~FOUO~~) How do we protect ourselves?

The best way to protect ourselves and our SIGINT is to play by the rules.

No matter how inconvenient the rules may seem, if we fail to adhere to them, the next set of rules will be far stricter.

(U//FOUO) There are very few things we cannot accomplish within the existing rules, using the authorities we have and those authorities we can receive.

(U//~~FOUO~~) Each phase of Production (collection, processing, retention, and dissemination) must be:

Accountable Defensible

Repeatable Retrievable

(C/) Violations of authorities must be reported:

1. at the time of recognition to SID O&C
2. as part of the E.O. 12333 quarterly report to the IG

(U//~~FOUO~~) If you determine that you have made a targeting mistake:

1. Stop the query as soon as possible
2. Notify your auditor

(S//SI//[redacted]) Anyone using NSA SIGINT databases must abide by the same rules and authorities as NSA.

Access to these databases is restricted to persons operating under DIRNSA authority.

(C// [redacted]) In addition to having a National Foreign Intelligence purpose (which includes FI, Counter-intelligence and Support to Military Operations), the following general rules apply:

(C// [redacted]) Additional authority is required to target:

- U.S. persons (anywhere) or people within U.S. territory

[redacted]

(C//   ) What is a Second Party Person?

In general terms, we apply the same basic definitions of a Second Party person as we apply for U.S. people.

U.S. Identities in SIGINT, Section 9 contains full definitions of each Second Party person.

(U//FOUO) End of Module 6

(U//FOUO) Module 7

Production Guidance

(U//~~FOUO~~) Targeting Clarifications

- Each query is an act of targeting.
- Start queries narrow; widen as necessary. Look out for queries that are too broad.
- Reasonableness, Not Perfection!



(U//~~FOUO~~) Targeting t

<u>end</u> via dictionaries

with follow-on querie

Choose qualifiers care

"**AND**" and "**BUT NOT**"

"**OR**" will expand your r

akes place <u>at front</u>

<u>**AND** at the keyboard</u>

es

fully

will reduce your results

eturns exponentially



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(S//SI// [redacted]) E-Mail Address Targeting

Specific e-mail addresses of valid foreign intelligence targets outside [redacted] countries may be targeted regardless of email domain without additional authority.

(S//SI//) E-Mail Address Targeting

Do Not:

<u>Wildcard domains</u>

<u>Wildcard user names</u>

<u>Wildcard across domains</u>

(S//)Dissemination Clarifications

E-mail addresses with U.S. domains may be included in dissemination if:

a. the user is a foreign national (excluding AUS/CAN/NZL/GBR)

b. Information is disseminated *only* to recipients who have a specific need for full addresses for a lawful government purpose.

(S//SI// [redacted]) Targeting Clarifications

Targeting:

- Permanently assigned?
- Check [redacted] Lookup tools BEFORE the first query
- Defeat domains using the same [redacted] but not a part of your target
- Do not wildcard

(S//SI//[redacted] Targeting Clarifications

Avoid general search terms without valid FI selectors

visa password narcotics
Bank

(Based on USSID SP0018, Sect. 5.1.c)

(S//SI//[redacted])

Sole Selectors

Targeting all communications on a given [redacted] will flood you with information that has no FI value or is to/from/about USPs

(S//SI//[redacted]) Avoid Site SIGADS as Sole Selectors

Do you need to see all information from a given site, or just select topics?

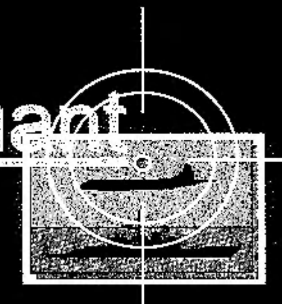
(S//SI//[redacted]) Avoid Names as Sole Selectors

Use locations, associates, or activities to focus searches on your target and not just anyone with that same name

(C//SI// [redacted]) Targeting foreign flagged ships or aircraft located in US territorial waters or airspace:

-COMINT stops at 12nm without additional authority

- ELINT to coastline and beyond pursuant to USSID AP2231



CONFIDENTIAL//COMINT// 20291123

[redacted] allowed if specific FI selectors are used as well.

(ex: [redacted]

AND [redacted])

(C//[redacted]) Dissemination Clarifications

Equipment and product designators, such as [redacted], and brand names may be included in SIGINT reports, if the focus is on the *product*, not the manufacturer of the product.

(C//SI//[redacted] Targeting Clarifications

Targeting Deceased U.S. People or communications devices registered to them requires:

a. a VERY strong foreign intelligence purpose

b. mission driver

c. approval of the NSA OGC

(C//SI//) Targeting Deceased People or communications devices registered to them requires:

a. a VERY strong foreign intelligence purpose
b. mission driver
c. approval of the appropriate

(C//SI//) Dissemination Clarification

Can deceased protected persons be named in dissemination?

U.S. : YES

: NO

(S//SI//   ) DO NOT USE Raw Traffic repositories to verify the protected status of an entity.

(S//SI//) Protected entities listed by name or context in dissemination **<u>do not imply</u>** collection is authorized.

(C//[redacted]) Imminent Threat to Safety

COLLECTION: USSID SP0018, 4.1.d.(1)

DIRNSA may authorize the collection to, from, or about a USP outside the U.S. when life or physical safety is reasonably believed to be in immediate danger.

Contact NSOC

(C// [redacted]) Dissemination Clarification

DISSEMINATION: USSID SP0018, 7.2.c.(6)

Information indicates that the identity of the USP is pertinent to a possible threat to the safety of any person or organization, including those who are targets, victims or hostages of international terrorist organizations.

(C//[redacted]) Dissemination Clarification

If a person is in imminent danger and you have relevant information, you may disseminate that information unmasked in product and follow-up with SV afterwards.

(C//[redacted]) Why do we still need this level of oversight?

Past Abuses	Present Examples
[redacted] targeting of international telegrams	[redacted] targeting of [redacted]

(C//) Why do we still need this level of oversight?

Past Abuses	Present Examples
Phone lines into the U.S. for identities of U.S. based narcotics smugglers	Restaurant in Texas to identify narcotics smuggler

(C//[redacted]) Why do we still need this level of oversight?

Past Abuses	Present Examples
Watch-listing U.S. people for evidence of foreign influence	Unauthorized targeting of suspected terrorists in U.S.

(U//~~FOUO~~) End of Module 7

(U//FOUO) Module 8

Dissemination Guidance

(U//~~FOUO~~) U.S. location identifiers in reports

Some US identifiers may be included when used in a LOCATIONAL SENSE (i.e. They identify a *place*).

- **RESTAURANTS**
- **HOTELS**
- **AIRLINE FLIGHT NUMBERS**
- **AIRPORTS**

(U//~~FOUO~~) Avoid Contextual Identification

Don't provide so much detail about a masked protected identity that the reader could determine who is being referenced due to context.

(C// [redacted]) Dissemination Authority

Generally, to include the identity of a U.S. person or entity in SIGINT product (by name, title, or context):

1) it must be necessary to understand or assess the foreign intelligence, and

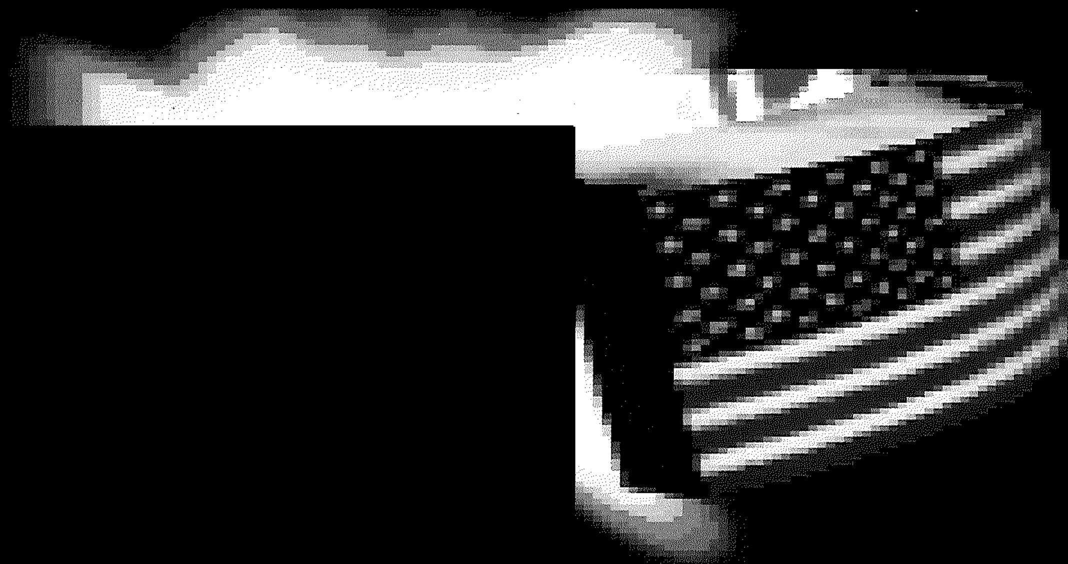
2) the recipient must need that information to perform his/her official duties.

3) You will need the approval of Chief Information Sharing Services.

4) Keep your focus on the foreign intelligence.

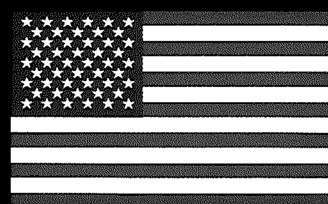
(U//FOUO) End of Module 8

(C//)



No chaining from or through U.S. contacts (email, phone, etc.)

Contacts Masked



(U//FOUO)

(S//SI//[redacted]) Why do U.S. SIGINT analysts care?

(S//SI//[redacted]) Tasking must comply with USSID SP0018 and [redacted].

(U//FOUO) End of Module 9